

Genuine randomness from an incoherent source

Bing Qi^{1,2,*}

¹Quantum Information Science Group, Computational Sciences and Engineering Division,
Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA

²Department of Physics and Astronomy, The University of Tennessee, Knoxville, TN 37996 - 1200, USA
(Dated: November 2, 2016)

Quantum random number generators (QRNGs) harness the intrinsic randomness in measurement processes: the measurement outputs are truly random given the input state is a superposition of the eigenstates of the measurement operators. We show in the case of *trusted* devices, genuine randomness could be generated even when the input to the detector is a mixed state. We propose a random number generation scheme based on measuring the quadrature fluctuations of a single mode thermal state with an optical homodyne detector. By interfering a broadband incoherent source with a single mode local oscillator at a beam splitter and performing differential photodetection, we can selectively detect the quadrature fluctuations of a single mode of the incoherent source, thanks to the “filtering” function introduced by the local oscillator. Experimentally, a quadrature variance about three orders of magnitude larger than the vacuum noise is observed from an amplified spontaneous emission source, suggesting this scheme can tolerate much high technical noises in comparison with QRNGs based on measuring the vacuum noise. The high quality of this entropy source is evidenced by the small correlation coefficients of the acquired data. ^a

PACS numbers: 03.67.Dd, 05.40.-a

I. INTRODUCTION

Quantum random number generation is an emerging technology [1, 2], which has great impacts in both fundamental researches [3] and practical applications. Different from other types of physical random number generator exploring chaotic behaviors of classical deterministic systems, a quantum random number generator (QRNG) harnesses the truly probabilistic nature of fundamental quantum processes [4, 5].

In general, quantum random number generation can be divided into two steps: the measurement step and the randomness extraction step. In the first step, a well-defined measurement is performed on the output of an entropy source. According to Born’s rule [6], if the quantum state arrived at the detector is a superposition of the eigenstates of the measurement operators, the measurement outputs are truly random. Ideally, the measurement system should only detect the *intrinsic* quantum noise. In practice, both the entropy source and the detection system are not perfect and will introduce additional technical noises. Very often, it is difficult to identify and fully characterize all the sources of the technical

noises. In the worst case of scenario, the technical noises could be accessible to a malicious adversary (Eve) and thus are *untrusted*. The second step in random number generation is to remove the correlation between the final random bits and the untrusted technical noises by performing randomness extraction. This step typically involves an estimation of the amount of available quantum entropy, followed by an application of hashing functions to generate truly random number from raw data [7–10]. Since the randomness extraction schemes are more or less universal and have been well studied and demonstrated in various QRNG schemes [10–14], in this paper, we will only discuss the first step in random number generation: to develop a good entropy source.

Among various implementations, QRNG based on photonic technology has drawn a lot of attention for its high rate, low cost and the potential of chip-size integration [15, 16]. Both single photon detectors and optical homodyne detectors have been employed in photonics QRNG. The latter is especially appealing in practice since highly efficient photo-diodes working at room temperature can be applied. Several QRNG schemes based on optical homodyne detection, exploring fundamental noises such as vacuum fluctuation [17–20] and laser phase noise [21–24], have been studied extensively. Remarkably, QRNG based on laser phase noise has been employed in a recent loop-hole free Bell experiment [25].

In this paper, we propose a random number generation scheme based on measuring the quadrature fluctuations of a single mode thermal state with an optical homodyne detector. This scheme can be implemented by interfering a broadband incoherent source with a single mode local oscillator (LO) at a symmetric beam splitter and performing differential photodetection. Our scheme can tolerate much high technical noises in comparison with

* qib1@ornl.gov

^a This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (<http://energy.gov/downloads/doepublic-access-plan>).

QRNG based on measuring the vacuum noise. This is because the quadrature variance of a single mode thermal state with an average photon number of n is $2n + 1$ times as large as that of vacuum state. By preparing a thermal state with a large n , we can effectively increase the *quantum noise-to-technical noise* ratio. Our scheme is also simpler than the one based on laser phase noise: both the incoherent source and the LO are operated in continuous-wave (cw) mode; no active modulation and phase (or polarization) stabilization are required. Our scheme is different from previous studies using broadband sources, where the main entropy source is the ASE-ASE beat noises [26, 27].

This paper is organized as follows: in Section II, we discuss random number generation from an incoherent source. In Section III, we present our experimental setup and results. Finally, we conclude this paper with a discussion in Section IV.

II. GENUINE RANDOMNESS FROM AN INCOHERENT SOURCE

At the first sight, it seems controversial to generate true randomness from an incoherent source since intrinsic randomness is deeply connected to quantum coherence [28]. Fig.1 (a) shows a representative QRNG scheme where a single photon is sent through a symmetric beam splitter and a pair of single photo detectors (SPDs) are employed to detect the photon. Based on which SPD fires, either bit 1 or bit 0 is generated. We can define the combination of the single photon source and the beam splitter as the entropy source, and the combination of the two SPDs as the detection system. In this case, the quantum state received by the detection system is a pure state given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}\{|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2\}, \quad (1)$$

where $|1\rangle_i$ and $|0\rangle_i$ represent single photon state and vacuum state at output port i ($i=1,2$). Note the state in (1) is a pure state. According to Born's rule, the measurement outputs are truly random.

If all the components in Fig.1 (a) are trusted and perfect (lossless and noiseless), then one of the SPDs becomes redundant: knowing the output of SPD₁ allows us to perfectly predict the output of SPD₂. So we can simplify the QRNG by removing SPD₂ and blocking the unused output port of the beam splitter (to make sure Eve cannot access it), as shown in Fig.1 (b). Based on whether SPD₁ detects a photon or not, either bit 1 or bit 0 is generated. If we define SPD₁ in Fig.1 (b) as the detection system, the accessible quantum state becomes a mixed state given by

$$\rho = \frac{1}{2}\{|1\rangle\langle 1| + |0\rangle\langle 0|\}, \quad (2)$$

where the label of path 1 has been neglected for simplicity.

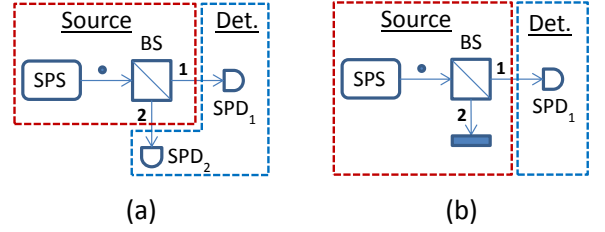


FIG. 1: A representative QRNG scheme. SPS—single photon source; BS—symmetric beam splitter; SPD_{1/2}—single photon detector. (a) The implementation using two SPDs, where the combination of the SPS and the BS is defined as the entropy source while the combination of two SPDs is defined as the detection system. In this case, the quantum state received by the detection system is a pure state. (b) The implementation using one SPD where the combination of the SPS and the BS is defined as the entropy source while SPD₁ is defined as the detection system. In this case, the quantum state received by the detection system is a mixed state. If all the devices are trusted and perfect (lossless and noiseless), the above two implementations are equivalent.

The equivalency of the above two schemes suggests, in the case of *trusted* device, genuine randomness could be generated from mixed states. The same argument can also be applied to QRNGs based on radioactivity [29] or based on laser phase noise due to spontaneous emission [21–24], where the emitted electrons or photons accessible to the detector are in mixed states.

A practical incoherent source, such as a superluminescent diode (SLD) or an optical amplifier, is a more complicated system. Nevertheless, the quantum state of the whole system, including the light source and the emitted photons, can be treated as a pure state. Same as the example given in Fig.1, genuine randomness could be generated by measuring only the emitted photons as long as Eve cannot access the light source.

III. EXPERIMENTAL SETUP AND RESULTS

We propose a random number generation scheme based on measuring the quadrature fluctuations of a single mode thermal state with an optical homodyne detector. The experimental setup is shown in Fig.2. The amplified spontaneous emission (ASE) source is an optical amplifier (PriTel, Inc.) with vacuum state input. A 0.8nm optical bandpass filter centered at 1542 nm is placed after the ASE source. The filter can reduce the power of unused light arrived at the detector and facilitate the estimation of the photon number per mode. The attenuated output (about 4 mW) of a laser source (Clarity-NLL-1542-HP from Wavelength Reference), whose central wavelength is within the above 0.8nm range, is employed as the LO.

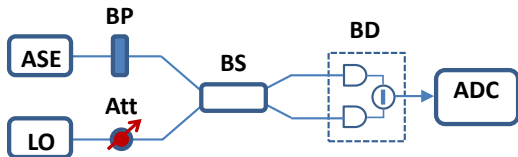


FIG. 2: Experimental setup. ASE—amplified spontaneous emission source; LO—local oscillator; BP—optical bandpass filter; Att—variable optical attenuator; BS—fiber beam splitter; BD—balanced photoreceiver; ADC—analog-to-digital converter.

The interference signals after the 50:50 fiber beam splitter are measured with a 350MHz balanced photoreceiver (Thorlabs). Note all the components used in the experiment have single mode fiber connectors. Both the ASE source and the LO laser are operated in cw mode. No polarization control or phase stabilization are required.

The optical power of the filtered, unpolarized ASE light is measured to be $29.0\mu w$, which can be translated into an average photon number $n \sim 500$ per spatialtemporal and polarization mode. This suggests that the expected quadrature variance of this source is about three orders of magnitude ($2n + 1$) larger than the vacuum noise, a significant advantage of our scheme.

We should emphasize that although the output of the ASE source is multimode, the optical homodyne detector only detect signals in the same mode as the LO. This “filtering” function of the LO allows us to perform single mode measurement without actually preparing a single mode thermal state.

In the first experiment, a 12-bit data acquisition board (Texas Instruments) was employed to sample the output of the balanced photoreceiver at a sampling rate of 100MHz. This sampling rate is mainly limited by the bandwidth of the detector. Limited by the memory size of the data acquisition board, 10^5 samples were collected in this experiment. The histogram of the acquired data is shown in Fig.3. As expected from a single mode thermal state, the quadrature distribution fits a Gaussian function reasonably well. The variance of the acquired data has been determined to be 960 in the shot-noise unit, which is in good agreement with the expected value of $2n + 1$ with $n \sim 500$.

In the second experiment, an 8-bit oscilloscope (Agilent) was used to acquire 10^7 samples at a sampling rate of 100MHz. The autocorrelation of the collected data is shown in Fig.4. The correlation coefficients are very small and within the range of the statistical uncertainty due to the finite sample size.

IV. DISCUSSION

In summary, we propose and demonstrate a photonic entropy source for randomness generation based on mea-

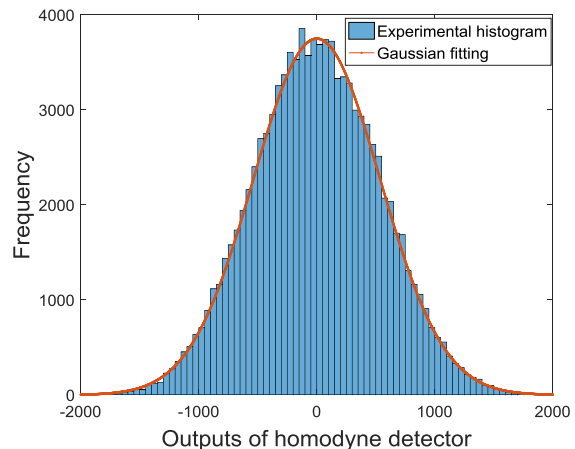


FIG. 3: Histogram of the measurement results and a Gaussian fitting curve. Sample size= 10^5 .

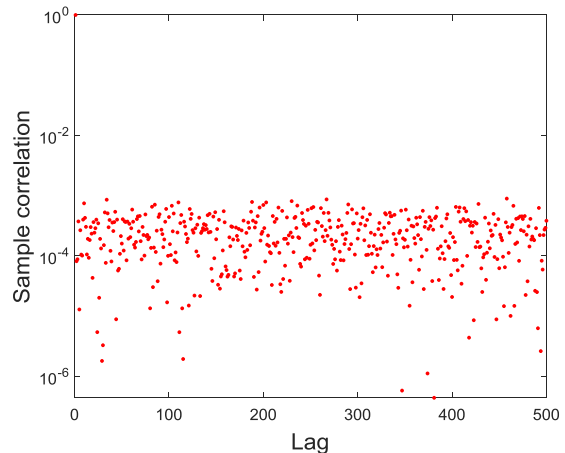


FIG. 4: Autocorrelation of Samples. Sample size= 10^7 .

suring the quadrature fluctuations of incoherent light using optical homodyne detection. Similar to the case of QRNG based on vacuum noise, the random numbers generated by our scheme follow a Gaussian distribution, which are on demand in applications like the Gaussian-Modulated Coherent States quantum key distribution [30].

One important advantage of our scheme is its simple design: both the incoherent source and the LO are operated in cw mode; no active modulation and phase (or polarization) stabilization are required. Experimentally, a quadrature variance about three orders of magnitude larger than the vacuum noise is observed, suggesting this scheme can tolerate much high technical noises in comparison with QRNG based on measuring the vacuum noise. The high quality of this entropy source is evidenced by the small correlation coefficients of the acquired data. To further generate genuine random num-

bers, existing randomness extraction schemes can be applied [7, 8, 10].

This work was performed at Oak Ridge National Laboratory (ORNL), operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-

00OR22725. The authors acknowledge support from ORNL laboratory directed research and development program (LDRD), the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDs) program under contract M614000329, and the U.S. Office of Naval Research (ONR).

-
- [1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, *npj Quantum Inf.* **2**, 16021 (2016).
 - [2] M. Herrero-Collantes and J. C. Garcia-Escartin, arXiv:1604.03304v1 (2016).
 - [3] B. Hensen, et al., *Nature* **526**, 682 (2015).
 - [4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *Rev. Sci. Instrum.* **71**, 1675 (2000).
 - [5] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, *J. Mod. Opt.* **47**, 595 (2000).
 - [6] M. Born, *Z. Phys.* **37**, 863 (1926).
 - [7] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, *Phys. Rev. A* **87**, 062327 (2013).
 - [8] D. Frauchiger, R. Renner, and M. Troyer, arXiv:1311.4547 (2013).
 - [9] P. Lougovski and R. Pooser, arXiv:1404.5977 (2014).
 - [10] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, *Phys. Rev. Applied* **3**, 054004 (2015).
 - [11] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Opt. Express* **20**, 12366 (2012).
 - [12] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, *Opt. Express* **22**, 1645 (2014).
 - [13] M. W. Mitchell, C. Abellán, and W. Amaya, *Phys. Rev. A* **91**, 012314 (2015).
 - [14] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, *Rev. Sci. Instrum.* **86**, 063105 (2015).
 - [15] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermann, *IEEE Photon. J.* **7**, 113 (2015).
 - [16] C. Abellán, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, *Optica* **3**, 989 (2016).
 - [17] A. Trifonov and H. Vig, *United States Patent* 7284024 (2007).
 - [18] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerner, U. L. Andersen, C. Marquardt, and G. Leuchs, *Nature Photonics* **4**, 711 (2010).
 - [19] Y. Shen, L. Tian, and H. Zou, *Phys. Rev. A* **81**, 063814 (2010).
 - [20] T. Symul, S. M. Assad, and P. K. Lam, *Appl. Phys. Lett.* **98**, 231103 (2011).
 - [21] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, *Opt. Lett.* **35**, 312 (2010).
 - [22] H. Guo, W. Tang, Y. Liu, and W. Wei, *Phys. Rev. E* **81**, 051137 (2010).
 - [23] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, *Opt. Express* **19**, 20665 (2011).
 - [24] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, *Appl. Phys. Lett.* **104**, 261112 (2014).
 - [25] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, *Phys. Rev. Lett.* **115**, 250403 (2015).
 - [26] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, *Opt. Express* **18**, 23584 (2010).
 - [27] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, *Opt. Lett.* **36**, 1020 (2011).
 - [28] X. Yuan, H. Zhou, Z. Cao, and X. Ma, *Phys. Rev. A* **92**, 022124 (2015).
 - [29] M. Isida and Y. Ikeda, *Ann. Inst. Stat. Math.* **8**, 119 (1956).
 - [30] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, *Nature* **421**, 238 (2003).